Hastings Communications and Entertainment Law Journal

Volume 30 | Number 3 Article 7

1-1-2008

The Federal Communications Commission and the NSA Call Database: The Duty to Investigate

Alan J. Chang

The Federal Communications Commission and the NSA Call Database: The Duty to Investigate

by
ALAN J. CHANG*

I. Introduction

On May 10, 2006, *USA Today* revealed an intriguing controversy that sparked the curiosity of the American public.[1] According to the report, the

* J.D. Candidate, University of California, Hastings College of the Law, 2008; B.S. University of Illinois at Champaign-Urbana, 2005. Special thanks to Professor Aaron Rappaport for contributing feedback to this Note.

United States National Security Agency ("NSA") purportedly created its own call database[2] that consisted of consumers' private phone records from four of the largest telephone companies in the United States: AT&T, BellSouth, Verizon, and SBC.[3] Furthermore, the phone companies' affiliation with constructing the NSA Call Database could potentially be illegal under United States law.[4]

After news of the database became public knowledge, members of Congress called for a Federal Communications Commission ("FCC") investigation to determine whether those companies broke the law.[5] Following internal disagreement among its representatives, the FCC ultimately declined to investigate or impose regulations on the telecommunications providers due to the "classified nature of the [NSA Call Database]."[6] Specifically, the commission claimed that disclosing any information would "cause exceptionally grave damage to the national security of the United States."[7] In turn, the FCC's refusal to involve itself in this matter has led to much criticism by the government and public alike.[8]

If the FCC is the government agency directly in charge of regulating all facets of citizens' communication, why did they decline to look into this potential breach of consumer privacy? At the same time, is an FCC investigation necessary to determine potential issues of legality concerning the NSA Call Database, as opposed to leaving the matter strictly for the U.S. federal courts? This note will outline and analyze the substantive law and policy regarding the FCC's role regarding the NSA Call Database. The NSA Call Database could potentially affect hundreds of millions of U.S. citizens' expectation of privacy, civil rights, and ability to rely on the government. Overall, the legal authority and policy tend to favor the need for the FCC, as an overriding authority in telecommunications law with special expertise, to investigate the matter on behalf of Verizon, AT&T,

1. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (last visited Mar. 6, 2008).

2. *Id.*

3. *Id*

4. *Id.*

5. Press Release, Congressman Ed Markey, FCC Refuses to Investigate NSA Program, Predicting Likely Administration Road Blocks (May 23, 2006), http://markey.house.gov/index.php?option=content&task=view&id=1610&Itemid=12.

6. William M. Welch, *NSA Secrecy Makes Investigation Impossible, FCC Says*, USA TODAY, http://www.usatoday.com/news/washington/2006-05-23-fcc-nsa_x.htm (last visited Mar. 6, 2008).

7. *Id.*

8. *Id.*

SBC, and BellSouth's consumers regarding this potentially immense breach of consumer privacy.

II. Overview and History

A proper analysis of the NSA Call Database necessitates a general overview of the purpose and structure of the two affected governmental agencies: the National Security Agency and the Federal Communications Commission. Further, a brief history of the NSA Call Database is also necessary to appropriately comprehend the controversy it has caused.

A. Government Agencies

1. The National Security Agency (NSA)

The National Security Agency officially formed in November of 1952.[9] As part of the Department of Defense,[10] the agency is primarily responsible for collecting and analyzing foreign communications.[11] To promote the goal of national safety,[12] President George W. Bush authorized the NSA to eavesdrop on various forms of communication, including radio broadcasting by organizations and individuals, the Internet, telephone calls, and any other readily obtainable means.[13] Since the NSA operates both internationally and domestically,[14] their activities have the potential to invade U.S. citizens' privacy.[15]

According to Executive Order 12333,[16] the NSA's charter,[17] the agency can exert efforts to obtain information that it deems to be "foreign intelligence or counterintelligence,"[18] but it cannot "[acquire] information

9. National Security Agency, Introduction to History, http://www.nsa.gov/history/index.cfm (last visited Mar. 6, 2008).

10. National Security Agency, Introduction to NSA/CSS, http://www.nsa.gov/about/index.cfm (last visited Mar. 6, 2008).

11. National Security Agency, Mission Statement, http://www.nsa.gov/about/about00003.cfm (last visited Mar. 6, 2008).

12. *Id.*

13. *See* Peter Baker, *President Acknowledges Approving Secretive Eavesdropping: Bush Also Urges Congress to Extend Patriot Act*, WASHINGTON POST, Dec. 18, 2005, at A01, http://www.washingtonpost.com/wpdyn/content/article/2005/12/17/ AR2005121700456_pf.html.

14. National Security Agency, Frequently Asked Questions – About NSA, http://www.nsa.gov/about/about00018.cfm (last visited Mar. 6, 2008).

15. *See* Baker, *supra* note 13.

16. National Security Agency, Executive Order 12333 – United States intelligence Activities, Dec. 4, 1981, http://www.reagan.utexas.edu/archives/speeches/1981/120481d.htm (last visited Mar. 6, 2008).

17. *Id.* at 1.8.

18. *Id.* at 1.8(a).

concerning the domestic activities of United States persons."[19] Traditionally, the NSA relied on the FBI to collect information on foreign intelligence activities within the United States.[20] Further, the NSA's activities are meant to focus on "embassies and missions of foreign nations."[21]

2. The Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) is an independent government agency that reports directly to Congress.[22] Congressional Title 47 U.S.C. §§ 151 and 154 outline the commission's structure and duties.[23] Generally, the FCC regulates interstate and international broadcasting (radio and television), interstate telecommunications (wire, satellite, and cable), and all international communications that begin or end in the United States.[24] As a whole, the Bureau's responsibilities include processing applications for licenses and other filings; analyzing complaints, conducting investigations, developing and implementing regulatory programs, and taking part in hearings.[25] With regard to potential misconduct in the sale of phone records, the Enforcement Bureau would be in charge of enforcing FCC rules, orders, and the provisions of the 1934 Communications Act.[26] Specifically, major areas that the Enforcement Bureau handles are homeland security, local competition, public safety, and, importantly, consumer privacy and protection.[27]

B. The NSA Call Database

In the Southern District of New York's case *Mcmurray v. Verizon Communications Inc.*,[28] attorneys claimed that the NSA began to construct a phone record database as early as seven months prior to the September 11, 2001, terrorist attacks.[29] In full, the database has an estimated 1.9

19. *Id.* at 1.8(d).

20. *Id.*

21. *Id.* at 1.8(c).

22. Federal Communications Commission, About the FCC, http://www.fcc.gov/aboutus.html (last visited Mar. 6, 2008).

23. 47 U.S.C §§ 151 and 154 (2000).

24. *See* Federal Communications Commission, *supra* note 22.

25. *Id.*

26. *Id.*

27. *Id.*

28. Andrew Harris, *Spy Agency Sought U.S. Call Records before 9/11, Lawyers say*, BLOOMBERG, June 30, 2006, http://www.bloomberg.com/apps/news?pid=20601087&sid=abIV0cO64zJE&refer.

29. *Id.*

trillion call-detail records,[30] and is quite possibly the "largest database ever assembled in the world."[31] The U.S. government's use of this supposed database, however, is unknown.[32] Nonetheless, the database is likely linked to the "Terrorist Surveillance Program," which is a highly controversial NSA program that permits warrantless electronic surveillance on phone calls and other forms of communication that are linked to suspected terrorists and affiliates of Al Qaeda.[33] Unlike the Terrorist Surveillance Program, however, the Bush administration has neither confirmed nor denied the existence of this domestic call-record database.[34]

Government officials have criticized and disagreed with the NSA Call Database. For example, Rep. Edward Markey of the U.S. House of Representatives and the Seventh District of Massachusetts[35] stated,

> [t]he FCC, which oversees the protection of consumer privacy under the Communications Act of 1934, has taken a pass at investigating what is estimated to be the nation's largest violation of consumer privacy ever to occur. If the oversight body that monitors our nation's communications is stepping aside[,] then Congress must step in."[36]

On the other hand, FCC Chair Kevin Martin stated that White House Director of National Intelligence, John Negroponte, and NSA Lieutenant General Keith B. Alexander had warned him that, "disclosing information [in and of itself] about the alleged relationship between AT&T [and other phone companies] and the NSA could hurt national security."[37] As a whole, the conflict and general disagreement about the NSA Call Database deal with whether the government can enforce national security in light of American individuals' guaranteed right to privacy.

As a result of this alleged conspiracy with the NSA, the phone companies publicly responded in contradictory and somewhat vague press

30. Democracy Now, *Three Major Telecom Companies Help US Government Spy On Millions of Americans*, May 12, 2006, http://www.democracynow.org/article.pl?sid=06/05/12/1353225.

31. Cauley, *supra* note 1.

32. *See id.*

33. *See* Press Release, The White House, Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program (Jan. 22, 2006) http://www.whitehouse.gov/news/releases/2006/01/20060122.html.

34. BBC News, *Doubts Over US Phone Firms Data*, July, 1, 2006, http://news.bbc.co.uk/2/hi/americas/5135458.stm.

35. Congressman Edward Markey – Homepage, http://markey.house.gov (last visited Mar. 6, 2008).

36. *FCC Refuses to Investigate NSA Program, Predicting Likely Administration Road Blocks, supra* note 5.

37. Matthew Lasar, *Markey Criticizes FCC Chair for Refusing to Open Investigation on NSA/Phone Records Case*, March 23, 2006, http://www.lasarletter.net/drupal/node/96.

releases. AT&T representatives, for example, openly admitted that, "whatever [they] did, the government told [them] to."[38] Verizon and BellSouth spokesmen, on the other hand, initially denied involvement in creating the NSA Call Database.[39] Soon afterward, however, Verizon released an additional, subsequent public statement where they refused to either confirm or deny a relationship with the NSA.[40]

The NSA Call Database may or may not be legal, and thus far the matter remains unresolved. The existence, use, and production of the database could violate various provisions of federal law such as the Communications Act of 1934,[41] Communications Assistance Law Enforcement Act,[42] and Foreign Intelligence Surveillance Act.[43] Furthermore, a number of federal districts have dealt with claims involving this issue,[44] but precedent thus far is inconclusive. Thus, controversy surrounds the NSA Call Database, which directly affects American consumers and the public alike. Several issues therefore remain unanswered as to what the primary legal authority should regulate the program, as well as who should appropriately step in and make decisions on its legality.

III. Analysis: The FCC vs. The Courts

With so many legal issues seemingly left unaddressed, the two main potential sources to resolve the NSA Call Database controversy are the FCC and the United States Federal Court system. On one hand, the FCC, according to its bylaws, must investigate and correspondingly regulate potential and actual breaches in consumer privacy.[45] At the same time, however, the U.S. Federal Courts have historically possessed the role and duty to resolve constitutional cases or controversies, and "say what the law is."[46] Furthermore, the main issues here seem to deal with interpreting the United States Constitution, which is perhaps better suited for specific, case-

38. Press Release, Electronic Frontier Foundation, EFF Sues AT&T to Stop Illegal Surveillance, Jan. 31, 2006, http://www.eff.org/press/archives/2006/01/31.

39. Assoc. Press, *Verizon Says It Didn't Give NSA Phone Records*, MSNBC.com, May 17, 2006, http://www.msnbc.msn.com/id/12821609/.

40. News Release, Verizon Issues Statement on NSA and Privacy Protection (May 12, 2006), http://newscenter.verizon.com/press-releases/verizon/2006/page.jsp?item ID=29670741.

41. *See generally* 47 U.S.C. § 151 (2000).

42. *Id.* §§ 1001-1002.

43. *See generally* 50 U.S.C. §§ 1801-1811, 1821-29, 1841-46, and 1861-62 (2000).

44. *See, e.g.*, ACLU v. NSA/Central Sec. Serv., 438 F. Supp. 2d 754, 754 (E.D. Mich. 2006); *see* Mayer, Afran et al v. Verizon Commc'n, Inc., Complaint, http://cryptome. org/mayer-016.pdf (last visited April 3, 2008).

45. Federal Communications Commission, *supra* note 22.

46. Marbury v. Madison, 5 U.S. 137, 177 (1803).

by-case, in-court judicial decisions rather than an overarching FCC investigation and corresponding regulations.

The question remains as to why, or if, a broad FCC investigation is the best means to determine whether the phone companies broke the law, while the primary alternative is to allow individually affected plaintiffs to bring forth piecemeal cases in the U.S. Federal Court System. The remainder of this note will outline, compare, and contrast the FCC's ability to investigate and regulate the NSA Call Database controversy, with the Federal Courts' competence and duty to decide the matter. In the end, the FCC not only has the duty to investigate, but the expertise, discretion, and proper tools to optimally address the issue. The Commission should thus commence an investigation on behalf of Verizon, BellSouth, AT&T, and SBC's consumers.

A. Federal Law and the NSA Call Database

1. The Communications Act of 1934

The Communications Act of 1934, a United States Federal law, was enacted on June 19, 1934[47] and codified as Chapter 5 of Title 47 of the United States Code.[48] On January 3, 1996, the 104th Congress of the United States amended the Communications Act of 1934 with the Telecommunications Act of 1996,[49] which governs a large part of the telecommunications industry today.[50] The main purpose of the Communications Act of 1934 (as amended) was to regulate interstate and foreign communications by wire, radio, and other means.[51] One of the many important components of the Act is section 222—the Privacy of Customer Information—which states that the FCC ought to enforce consumer privacy as a top priority.[52]

Section 222 of Title 47 of the United States Code contains detailed provisions that are meant to protect U.S. consumers' rights, including their right to privacy.[53] For example, section 222(a) expressly states that "[e]very telecommunications carrier has a duty to protect the confidentiality or proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers,

47. Communications Act of 1934, 47 U.S.C. §§ 151 et seq., 609 (2000).

48. *Id.*

49. Telecommunications Act of 1996, 47 U.S.C. § 251 et seq. (2000), Pub. L. 104-104, 110 Stat. 56 (1996), available at http://www.fcc.gov/telecom.html (last visited Mar. 6, 2008).

50. *Id.*

51. 47 U.S.C. § 151 (2000).

52. *Id.* § 222.

53. *Id.*

including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[54] Unless required by law or through express consent of a customer, a telecommunications carrier is obligated to only use, disclose, or permit access to proprietary network information to serve customers or publish public directories.[55]

Regarding aggregate consumer information, such data can only be released to other carriers or persons on "reasonable and nondiscriminatory terms," or by "reasonable request."[56] Nonetheless, a telecommunications carrier may use the information to bill their customers, protect its own rights and property,[57] and protect the consumers themselves from "fraudulent, abusive, or unlawful use of, or subscription to, such services."[58] The Act also sets forth appropriate use of consumer information within databases.[59] Specifically, section 227(c)(3) focuses on the improper use of consumer telephone numbers in databases for purposes of solicitation.[60] Furthermore, consumers have the right to opt out of databases without charge, with privacy interests as the primary focus.[61]

The NSA Call Database potentially violates the 1934 Communications Act. Mainly, the four major telephone companies might have compromised section 222,[62] or the privacy of customer information due to their involvement with the NSA call database. The unresolved issues include whether the means by which the companies provided or sold the telephone records was necessary, reasonable, nondiscriminatory, fraudulent, improper, or abusive.

2. The Communications Assistance Law Enforcement Act (CALEA)

Congress passed the Communications Assistance Law Enforcement Act (CALEA) on October 25, 1994, and it became a valid amendment to the United States Code on January 1, 1995.[63] Congress passed CALEA to assist law enforcement in citizen surveillance through digital telephone networks.[64] Specifically, the Act required telephone service providers to

54. *Id.* § 222(a).
55. *Id.* § 222(c)(1).
56. *Id.* § 222(c)(3).
57. *Id.* § 222(d)(1)-(2).
58. *Id.* § 222(d)(2).
59. *Id.* § 222(e)
60. *Id.* § 227(c)(3).
61. *Id* § 227(c)(3)(C).
62. Cauley, *supra* note 1.
63. Federal Communications Commission, Communications Assistance for Law Enforcement Act (CALEA), http://www.fcc.gov/calea (last visited June 23, 2007); *see also* 47 U.S.C. § 1001 et seq. (2000).
64. *Id.*

allow law enforcement agencies to tap into telephone conversations and retrieve call detail records, while making it impossible for individual citizens to detect such activity.[65] In its own words, CALEA was meant to "amend title 18, United States Code, to make clear a telecommunication carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes."[66]

Like the Communications Act of 1934, CALEA also relates to the NSA Call Database. AT&T, Bellsouth, Verizon, and SBC allegedly provided the National Security Agency with their consumers' private records. Furthermore, the purpose and use of the database is currently unknown. Questions therefore remain as to whether Congress intended to include the NSA as a "law enforcement agency" under CALEA, and whether the NSA's use (presumably for national security alongside the Terrorist Surveillance Program) is part of what Congress intended to address when it amended Title 47.

3. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act ("FISA") of 1978 puts forth procedures regarding the physical and electronic surveillance of intelligence information between "foreign power[s]."[67] FISA is codified in 50 U.S.C. §§1801-1811,[68] 1821-29,[69] 1841-46,[70] and 1861-62,[71] but was amended by the USA Patriot Act of 2001[72] to include terrorism for groups that are not specifically supported by a foreign government.[73] For most purposes, "foreign powers" include a foreign government, any of its constituents that are not substantially composed of U.S. persons, any entity that a foreign government controls or directs, groups that engage in international terrorism, and foreign political organizations.[74]

The President, through the Attorney General, can approve electronic surveillance without a court order only if it is between foreign powers and has no substantial likelihood to interfere with a United States resident's privacy.[75] In turn, the FISA provisions that set forth guidelines and

65. *Id.*

66. H.R. 4922, 103rd Cong., 2d Sess. (1994), available at http://www.epic.org/privacy/wiretap/calea/calea_law.html (last visited Mar. 25, 2008).

67. 50 U.S.C. §1801(a), (f) (1994).

68. *See* 50 U.S.C. §§ 1801-1811 (1994).

69. *See* 50 U.S.C. §§ 1821-1829.

70. *See* 50 U.S.C. §§ 1841-1846.

71. *See* 50 U.S.C. §§ 1861-1863.

72. *See* 50 U.S.C. § 1801(a)(1).

73. *Id.*

74. 50 U.S.C. § 1801(a)(1)-(3), (4)-(5).

75. *Id.* § 1802(a)(1)-(3).

authorize electronic surveillance or physical searches without a court order specifically exclude this application to international terrorist groups.[76] Therefore, under the requirements of FISA, warrants are absolutely necessary to gather intelligence information with respect to terrorism or national security.[77] Such warrants are either granted or denied, *ex parte* and non-adversarial, by the United States Foreign Intelligence Surveillance Court.[78]

The NSA Call Database triggers FISA because the NSA gathered U.S. residents' private information without an official court order. FISA permits the government to survey intelligence information from foreign sources for purposes of terrorism or national security.[79] However, the NSA's actions are challengeable because Verizon, AT&T, BellSouth, and SBC provided *domestic* call-records, which most likely do not qualify as foreign intelligence information within the ambit of FISA. Even if the NSA acquired these records for the purpose of combating terrorism, FISA states that court orders are necessary if the manner of collection invades privacy. The NSA Call Database therefore puts this expectation of privacy at issue.

4. Federal Law: Applied

Due to the potential violations of the Communications Act of 1934, CALEA, and FISA, the FCC would have to investigate the matter, or the affected consumers of the phone companies' actions could pursue litigation for the federal courts to declare legal conclusions and rules on the matter. Overall, four factors determine whether courts or government agencies set forth legal authority. Those factors are: "1) whether the question at issue is within the conventional experience of judges or whether it involves technical or policy considerations within the agency's particular field of expertise, 2) whether the question at issue is peculiarly within the agency's discretion, 3) whether there exists a substantial danger of inconsistent rulings, and 4) whether a prior application to the agency [about a proposed investigation] has been made."[80] All four of these factors favor an FCC investigation over the federal judicial system's approach to properly assess the four aforementioned phone companies' involvement with the NSA Call Database.

76. *Id.*

77. *Id.*

78. *Id.*

79. *See* 50 U.S.C. §§ 1801-1811 (1994).

80. Nat'l Commc'n Ass'n, Inc. v. Am. Tel. and Tel. Co., 813 F. Supp. 259, 262-63 (S.D.N.Y. 1993) (citing RCA Global Commc'n, Inc. v. Western Union Tel. Co., 521 F. Supp. 998, 1006 (S.D.N.Y. 1981)).

First, the FCC is the best authority to regulate the NSA Call Database because this issue falls within the agency's "particular field of expertise."[81] As a general rule, government regulatory agencies traditionally have expertise to deal with "particularized areas of law,"[82] and should therefore be afforded with "discretionary flexibility."[83] "The Federal Communications Commission, [for example], is the administrative agency charged with expert skill and knowledge within the telecommunications industry. It was established by the Federal Communications Act of 1934, 47 U.S.C. § 151 et seq. (the Act) and pursuant thereto has a broad range of powers including regulation, investigation, adjudication, and enforcement."[84]

The FCC, since its inception, has dealt with regulating the telecommunications industry and would logically have decades of relevant experience as a result. Unlike federal court judges, FCC representatives would not evaluate the NSA Call Database through subjective legal reasoning. Instead, the agency could properly utilize decades of its representatives' experience, and the results of prior, perhaps similar telecommunications investigations for a more thorough and complete analysis. Thus, given the FCC's definitive and historic expertise, the FCC presumably has a great deal of idiosyncratic knowledge than individual federal court judges to handle phone companies' potential misconduct, and any consequent consumer privacy abuses.[85] An FCC investigation is therefore the preferable manner to address the NSA Call Database.

Secondly, the FCC is not only the "expert agency"[86] on telephone company regulation, but it also has vast discretion to regulate the telecommunications industry as well. Namely, the FCC "is most familiar with the technical and policy issues governing . . . phone service and is [therefore] best positioned . . . to address [those] questions."[87] Specifically, the FCC's enforcement bureau has the authority, ability, and resources to protect consumer rights in the field of telecommunications.[88] Although the Call Database triggers federal law, the FCC is not limited in its authority to act in the best interest of preserving the consumers' right to privacy. In

81. *Id.*

82. Kimberly Dee, *Delegation, Deference, and Deregulation: A 3-D Look of Video Dial Tone*, 9 ADMIN. L.J. AM. U. 817, 834-35 (1995).

83. *Id.*

84. Unimat, Inc. v. MCI Telecomm. Corp., No. 92-5941, 1992 U.S. Dist. LEXIS 19320 (E.D. Pa. Dec. 17, 1992).

85. *Id.*

86. MCI WorldCom Commc'n, Inc. v. Commc'n Network Intl, Inc., No. 01-762, 2001 U.S. Dist. LEXIS 15898, at *15 (E.D. Pa. Aug. 28, 2001).

87. *Id.*

88. Federal Communications Commission, *supra* note 22.

turn, the FCC not only has the duty, responsibility, and expertise to regulate the phone companies' questionable decisions, but the broad discretion to do so as well.

Third, the FCC is better equipped than the federal courts to attend to the NSA Call Database because unlike the courts, the FCC could "provide a uniform solution"[89] to all parties the database affected. "It would be impossible for the FCC to fulfill its function of regulating the . . . telephone market if numerous federal district courts also undertake to decide the substantial questions which directly or indirectly affect the position of the carriers within the market."[90] Given the FCC's unique ability to potentially set forth consistency and justice for all the phone companies' individually affected consumers, it should at least be the first step taken to resolve the NSA Call Database controversy.

The FCC is not only the more logical choice to resolve the database debate in terms of judicial efficiency, but the federal court system would produce inconsistent holdings because it must approach the issue on a piecemeal basis. The database affected up to 1.9 trillion consumers, and depending on a particular federal judge's views of national security versus the individual right to privacy, inconsistent holdings could very well ensue (much like Edward Markey and Kevin Martin's clashing opinions discussed earlier). A uniform solution through an FCC investigation, however, would address affected consumers' general needs at once, without leaving the legality or constitutionality of the NSA Database in question by varying, contradictory, or inconsistent holdings. Allowing the federal courts to deal with these cases one-by-one would merely disrupt what the FCC is simply better equipped to deal with. An FCC investigation would fairly, consistently, and uniformly deal with the NSA Call Database controversy, absent the risk of inconsistent holdings or remedies that the courts would present. Although the phone companies could ultimately challenge unfavorable FCC rulings in court, the results of an FCC investigation would not go unnoticed. The courts could consider and evaluate the FCC's prior findings and only proceed with litigation as needed. Either way, the result of an FCC investigation on the NSA Call Database would be fewer lawsuits and more uniformity.

Finally, an FCC investigation is appropriate because "a prior application to the agency has been made."[91] When news of the NSA Call

89. *MCI WorldCom Commc'n, Inc.*, No. 01-762, 2001 U.S. Dist. LEXIS 15898, at *15.

90. *Id.* (citing In re Long Distance Telecomm. Lit., 612 F. Supp. 892, 897 (E.D. Mich. 1985)).

91. *National Communications Ass'n Inc. v. American Telephone and Telegraph Company*, 813 F. Supp. 259, 262-63 (S.D.N.Y. 1993) (citing *RCA Global Communications, Inc. v. Western Union Tel. Co.*, 521 F. Supp. 998, 1006 (S.D.N.Y. 1981)).

Database became public knowledge, Congress initially filed an application with the FCC to investigate the matter.[92] Although the commission ultimately denied the request, Congress immediately reported the matter to the FCC before it even considered the courts as a viable solution.[93] Therefore, despite the FCC's refusal to intervene with the NSA's activities, Congress originally presumed that the FCC was indeed the proper entity to regulate this matter on consumer privacy, not the courts. This requirement of a "prior application"[94] therefore provides even more weight in favor of an FCC investigation rather than the federal judicial system. Overall, because of the FCC's expertise in telecommunications, discretion to regulate, the threat of inconsistent holdings, and Congress's prior application, an FCC investigation is the proper method to assess the NSA Call Database's legality.

Not only is the FCC the best instrument to evaluate the NSA Call Database under federal law standards, but the sparse case law that is currently available, pertaining to this database, also demonstrates the agency's finer position.

B. NSA Wiretapping: Cases

Following the FCC's refusal to attend to the call-record database, a number of litigants brought suit against the NSA in the federal courts.[95] The cases primarily alleged breaches of individual privacy, and sought relief against the NSA's Terrorist Surveillance Program and Call Database. *American Civil Liberties Union v. National Security Agency* and *Mayer, Afran et al* v. *Verizon Communications Inc.*[96] were suits filed pertaining to these programs.

1. American Civil Liberties Union v. National Security Agency (ACLU v. NSA)

American Civil Liberties Union v. National Security Agency (*ACLU v. NSA*) was filed on January 17, 2006,[97] in the United States District Court, Eastern District of Michigan.[98] The ACLU brought forth the suit on behalf of itself, the Council on American-Islamic Relations, Greenpeace Inc., the National Association of Criminal Defense Lawyers, and five affected

92. *Id.*

93. *Id.*

94. *Id.*

95. *See, e.g.*, ACLU v. NSA/Central Sec. Serv, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

96. *See* Mayer, Afran et al v. Verizon Commc'n, Inc., Complaint, http://cryptome.org/mayer-016.pdf (last visited April 3, 2008).

97. ACLU of Northern California: ACLU v. NSA, Jan. 17, 2006, http://www.aclunc.org/cases/landmark_cases/aclu_v.shtml.

98. *ACLU v. NSA*, 438 F. Supp. 2d 754.

individuals against the NSA's "Terrorist Surveillance Program"[99] and the NSA Call Database.[100] The plaintiffs collectively requested declaratory judgment and injunctive relief,[101] and argued that the court should find the programs unconstitutional and against federal law.[102]

On August 17, 2006, District Court Judge Anna Diggs Taylor held that the Terrorist Surveillance Program, pertaining to "international telephone and internet communications of numerous persons and organizations"[103] within the United States, was unconstitutional and illegal.[104] Therefore, she granted injunctive relief to the plaintiffs, pending appeal.[105]

In her 44-page opinion, Judge Diggs Taylor stated that the Terrorist Surveillance Program was unconstitutional.[106] Specifically, the program violated U.S. citizens' guaranteed constitutional rights protected by the First Amendment, Fourth Amendment, and the Separation of Powers.[107] Further, she held that the surveillance program violated the necessary statutory guidelines of FISA, which were meant to regulate intelligence agencies' access to private information.[108] However, Judge Diggs Taylor did not rule on the alleged NSA database of domestic call detail records,[109] citing the States Secrets Privilege.[110]

2. Mayer, Afran et al. v. Verizon Communications, Inc.

On May 12, 2006, Carol J. Mayer and Bruce I. Afran, citizens of New Jersey, brought a class action suit against Verizon, the NSA, and George W. Bush based on allegations involving Verizon's contributions to the NSA Call Database.[111] This case was based upon Verizon violating the

99. *Id.*

100. ACLU v. NSA Complaint for Declaratory and Injunctive Relief, available at http://www.aclu.org/images/nsaspying/asset_upload_file137_23491.pdf (last visited Jan. 20, 2007).

101. *Id.*

102. *ACLU v. NSA*, 438 F. Supp. 2d at 758.

103. *Id.*

104. *Id.* at 782.

105. *Id.*

106. *Id.*

107. *ACLU v. NSA*, 438 F. Supp. 2d at 782. The Separation of Powers promises that each branch of the state (executive, legislative, and judicial) has separate and independent powers and areas of responsibility with the goal of preventing tyranny.

108. *ACLU v. NSA*, 438 F. Supp. 2d at 782.

109. *Id.* at 759.

110. *Id.* The State Secrets Privilege is an evidentiary rule that allows the federal government to prevent the disclosure of information which is potentially detrimental to national security in legal proceedings.

111. Mayer, Afran Complaint, *supra* note 44.

First Amendment, Fourth Amendment, and the Telecommunications Act of 1996 (the latest amendment to the Communications Act of 1934).[112]

Although the purpose of the database is asserted to be for monitoring terrorist networks and telephone calling patterns, the complaint alleged that these activities were based on no warrants, no suspicion of terrorist activity, and no probable cause of criminal activity.[113] Plaintiffs further alleged that without a proper warrant under FISA or subscriber consent, such activities are illegal.[114] President Bush himself was also a named defendant in this case for violating U.S. Citizens' expectation of privacy in telephone communications under the First Amendment.[115] The plaintiffs sought declaratory relief, an injunction, and monetary damages of $1,000 per violation, which amounted to a minimal collective amount of $5,000,000,000.[116] Based on the numbers, Verizon's supposed phone sales affected at least 5,000,000 class members. As of this note, the presiding court has yet to render a decision on this case.

3. Wiretapping Cases: Applied

Although a handful of plaintiffs have attempted to seek relief in the federal court system, the results of *ACLU v. NSA* and *Mayer, Afran et al. v. Verizon Communications Inc.* demonstrate that the NSA Call Database has not been sufficiently handled. *ACLU v. NSA*, for example, failed to even address the NSA Call Database, although it was a primary allegation in the plaintiff's case. The pending case *Mayer, Afran et al. v Verizon Communications, Inc.* is directly on point, and was brought against the NSA Call Database itself. However, plaintiffs only named Verizon as a defendant in the action, because they only had a cause of action against the company that handed over their private phone records. In turn, this leaves AT&T, BellSouth, and SBC's affiliation with the database uncertain, which the FCC, however, would address with a proper investigation. Cases similar to *Mayer* could be brought one at a time by the other companies' consumers. However, for the reasons outlined in Section III(A), this approach would simply be far less efficient, effective, and accurate than an FCC investigation. Considering the vast likelihood of inconsistent holdings, the FCC's expertise, and the agency's inherent discretion in regulating matters within the telecommunications sector, an FCC investigation simply makes sense.

112. *Id.* at ¶ 10.
113. *Id.* at ¶ 13.
114. *Id.* at ¶ 126.
115. *Id.* at ¶ 124.
116. Mayer, Afran Complaint, *supra* note 44, at ¶ 130.

Importantly, however, federal judges have the well-established, historic duty to resolve matters concerning American individuals' civil and constitutional rights.[117] Judge Diggs Taylor in *ACLU v. NSA*, for example, fulfilled this role and held that the Terrorist Surveillance Program was unconstitutional.[118] However, unlike the Terrorist Surveillance Program, the NSA Call Database differs from direct conflicts between government agents and individuals within the United States who assert and defend their constitutional right to privacy. The NSA Call Database involves large, powerful, non-governmental third party telecommunications companies that allegedly sold trillions of phone records held by service providers. According to the FCC's charter and purpose, oversight of potential misconduct regarding such breaches in consumer privacy falls directly within the province of the FCC.[119]

A great deal of inconclusive information thus remains concerning the NSA Call Database, the companies' involvement, and how the NSA utilizes this system. However, the heart of the matter that requires FCC involvement is in determining any potential misconduct by AT&T, BellSouth, Verizon, or SBC when they allegedly provided information in a manner that violated consumer privacy. The FCC, as opposed to individual plaintiffs as litigants, has more significant resources, funding, expertise, and discretion to evaluate the phone companies' actions than any individual or plaintiff class could set forth in front of a federal court judge. Investigations over the United States' communications sector is precisely what the FCC was created for in 1934, and is funded to do today. Therefore, an FCC investigation is the most sensible approach in determining the legality, or lack thereof, of the companies' potential impropriety.

IV. Conclusion

The FCC is the authority and regulatory agency concerning telecommunications. Hence, the commission is the proper entity to settle the debate and make a decision as to whether the NSA Call Database is constitutional. Although AT&T, BellSouth, Verizon, and SBC might have assisted the government for the purpose of national security, the FCC is nonetheless meant to regulate telecommunication carriers to foster confidentiality and the safe flow of information. To allow the judicial system to settle this matter without intervention from the FCC would result in a less effective, less efficient, and therefore impractical approach to

117. *See generally* 47 U.S.C. §151 (2000).

118. *See* ACLU v. NSA/Central Sec. Serv, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006).

119. *See* Federal Communications Commission, *supra* note 22.

resolve the consumers' rightful concerns. For that reason, an FCC investigation is not only the appropriate legal measure to pursue, but it is also the most sensible step to take. Until then, numerous American consumers are left waiting.

* * *